IMPLEMENTING A NET-CENTRIC DATA ACCESS SERVICE

December 2007

A White Paper

Mary K. Pulvermacher, The MITRE Corporation

ABSTRACT: The United States Department of Defense (DoD) has a well documented desire to evolve toward network-centric information sharing as a means to achieve effective military and government operations. Net-centric information sharing entails making data and services visible, accessible, understandable, trusted and governable to known and unanticipated users on a network. Actions to implement net-centric data and services are captured in DoD and Intelligence Community (IC) net-centric strategies. This paper provides a suggested approach for implementing net-centric data access services in accordance with these strategies.

Table of Contents

Implementing a Net-Centric Data Access Service

A WHITE PAPER

WHY THIS PAPER?

A recent corporately funded MITRE and Aerospace initiative to implement a prototype as a pathfinder for net-centric information sharing in the Military Satellite Communications (MILSATCOM) domain reinforced the MITRE and Aerospace team's belief that a greater understanding of what it means to build a net-centric service is needed. Therefore, we decided it would be valuable to capture and share a short summary of the process we had planned to use to implement this net-centric pathfinder. Our cross-corporate team heavily leveraged other relevant experience to include deep domain knowledge as well as past experience implementing net-centric data access services as part of the inaugural Command and Control (C2) Space Situational Awareness (SSA) Community of Interest (COI) pilot.[1] This paper also heavily leverages the Department of Defense (DoD) Deputy Chief Information Officer (DCIO) sponsored DoD Net-Centric Data Strategy and COI training. [5] This MITRE developed training incorporates the experiences and lessons learned from many COI initiatives. Senior officials from across the military services have attended this training in 2007[2].

Members of the MITRE and Aerospace MILSATCOM Situational Awareness (SA) Initiative Team include:

- **Initiative Leads**: Mr. Jeff J. Ansted (Aerospace) and Ms. Mary K. Pulvermacher (MITRE)
- **Human Systems Integration Experts**: Ms. Janet Perron (MITRE) and Mr. Todd Reily (MITRE)
- **Initiative Development Team**: Mr. Paul Franklin (MITRE), Mr. Adam Gruca (MITRE) and Ms. Maryann Hutchison (Aerospace)

PAPER CONTENTS

This paper begins by describing the importance of a net-centric approach. It then introduces Core Enterprise Services that may be used to help implement net-centric services. The next section suggests using a COI pilot as a pathfinder for implementing net-centric services. Finally, we outline

[1] For more information on the C2 SSA COI pilot, see the C2 SSA COI Community of Practice site at https://rso.my.af.mil/afknprod/ASPs/CoP/ClosedCoP.asp?Filter=OO-OT-SP-03 Note that you need an Air Force Knowledge Now (AFKN) account to access this site. Go to ww.my.af.mil to register for a AFKN account.

[2] For inquiries regarding the DoD Data Strategy / Community of Interest (COI) training, email the DCIO office at: COI_HelpDesk@osd.mil

recommended steps for implementing a net-centric data access service. These steps assume that the services make data available from an authoritative source for that data.

WHY A NET-CENTRIC APPROACH?

The importance of a network centric approach is well documented across the DoD. Here are but a few quotes that capture the need for a net-centric approach to support effective military and government operations.

- “Defense transformation hinges on the recognition that information is our greatest source of power.” [8]
- “Ensuring timely and trusted information is available where it is needed, when it is needed, and to those who need it most is at the heart of the capability needed to conduct Network-Centric Operations (NCO).” [8]
- “We will conduct network-centric operations with compatible information and communications systems, usable data, and flexible operational constructs.” (National Defense Strategy 2005)
- “The hallmark of the 21st century is uncertainty. Net-Centricity is rooted in a simple principle: Confront uncertainty with agility. To be agile, data can no longer be “owned”…it must be shared.” [8]

The good news is that the DoD has developed an approach for net-centric information sharing. DoD Directive 8320.2 directs the implementation of data sharing in accordance with the DoD Net-Centric Data Strategy. [4] The DoD Net-Centric Data Strategy outlines a vision for managing data in this net-centric environment. Key components of this data strategy are to make data visible, accessible, understandable, trusted, and governable, as shown in figure 1.

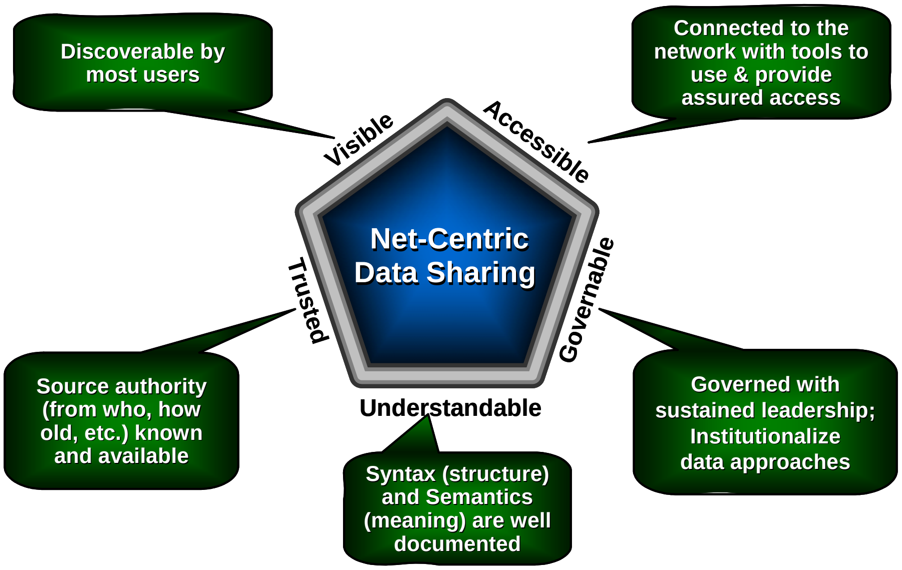
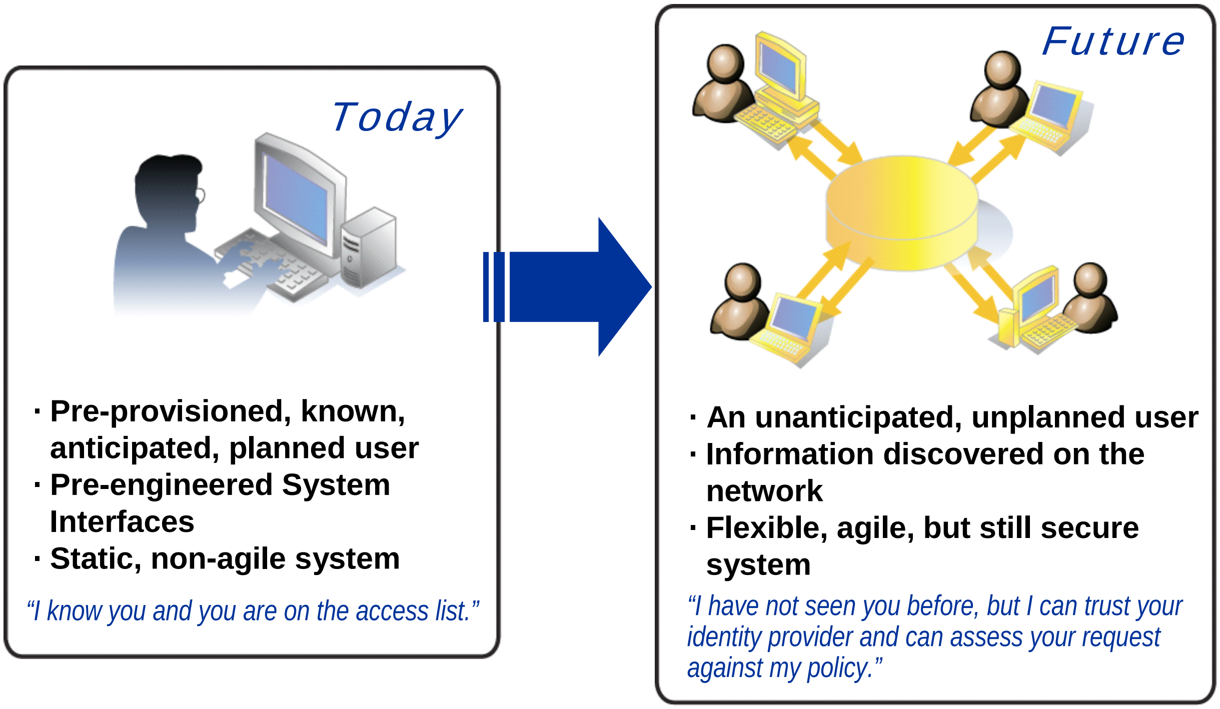

Discoverable by most users
Connected to the network with tools to use & provide assured access
Visible
Accessible
Net-Centric Data Sharing
Trusted
Governable
Understandable
Source authority (from who, how old, etc.) known and available
Syntax (structure) and Semantics (meaning) are well documented
Governed with sustained leadership; Institutionalize data approaches

FIGURE 1. KEY COMPONENTS OF DOD NET-CENTRIC DATA STRATEGY

The data strategy states that net-centricity compels a shift to a “many-to-many” exchange of data, enabling many users and applications to leverage the same data—extending beyond the previous focus on predefined, point-to-point interfaces. Implementing this strategy makes data available to known users while also allowing unanticipated but authorized users or applications to find and use data more quickly. This need for a flexible, agile, and secure system is embodied in figure 2[3].

The more recent DoD and Intelligence Community (IC) Net-Centric Services Strategy [6] describes the DoD’s vision for establishing a net-centric environment that increasingly leverages shared services and Service Oriented Architecture (SOA). This services strategy expands upon the DoD Net-Centric Data Strategy by connecting services to the Data Strategy goals.



- Pre-provisioned, known, anticipated, planned user
- Pre-engineered System Interfaces
- Static, non-agile system

“I know you and you are on the access list.”

- An unanticipated, unplanned user
- Information discovered on the network
- Flexible, agile, but still secure system

“I have not seen you before, but I can trust your identity provider and can assess your request against my policy.”

FIGURE 2. SECURE NET-CENTRIC INFORMATION SHARING

Conclusion: A net-centric approach is an essential component of achieving effective military and government operations. Adopt and implement a net-centric approach.

[3] Source: 2007 C4ISR Integration and interoperability Report, The MITRE Corporation, November 2007 DRAFT

NET-CENTRIC CORE ENTERPRISE SERVICES PROGRAM

To facilitate the DoD's goal of implementing net-centric information sharing, the Defense Information Systems Agency (DISA) is providing a set of Core Enterprise Services (CES) through its Net-Centric Enterprise Service (NCES) program. [7] The NCES program provides a common foundation for capabilities needed by many programs. Using NCES saves programs from implementing the capabilities themselves and provides a common foundation across the DoD, federal government, and beyond. The NCES Program offers capabilities that are designed to interact with each other through a Services Oriented Architecture (SOA) approach. Applications that wish to use NCES services do so through well defined interfaces in accordance with SOA principles.

The CES will allow users and information systems to:

- Find and access relevant information;
- Expose the information they produce for others to discover;
- Collaborate in a more effective manner;
- Distribute data to forward deployed areas;
- Increase performance and reliability of data access, and;
- Utilize the enterprise infrastructure for evolving DoD systems to a Service-Oriented Architecture.

NCES is making available the following capabilities on the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet) at no charge:

- Portal
- Service Security
- Mediation
- Content Discovery
- Content Delivery
- Service Discovery
- Machine-to-Machine Messaging
- Metadata Discovery
- Enterprise Catalog

The NCES program represents a different approach for the DoD—an approach that is market-based, enterprise-wide, and joint by design. NCES customers are intended to include the warfighter, intelligence, and business domains—anyone within the DoD community who needs to share and retrieve information. Thus, the NCES program is an enabler for information sharing within the DoD as well as with federal, allied, coalition and multinational partners.

Conclusions: NCES is essential to the Department's ability to implement a network-based information environment that will meet the requirement for information and decision superiority. NCES will provide the core enterprise services that programs and Community of Interest capabilities developers will use in the development of mission applications.

CONSIDER A COMMUNITY OF INTEREST (COI) PILOT

The DoD Net-Centric Data Strategy introduces the concept of management of data within a Community of Interest (COI). A COI is "A collaborative group of users that must exchange information in pursuit of its shared goals, interests, missions, or business processes and therefore must have shared vocabulary for the information exchanges." [1] Several COIs exist, and more are forming, to solve mission-specific information sharing problems affecting their communities. These COIs are intended to increase information sharing volume, speed, and reach to known and unanticipated users. They also provide a user forum to drive the net-centric approach forward and foster collaboration within and across communities. Successful COIs have engaged executive leadership which provides the authority to solve the information sharing problem. Most COIs begin by launching a pilot to serve as a pathfinder for net-centric information sharing.

One of the most successful COIs is the Maritime Domain Awareness (MDA) Data Sharing (DS) COI. This COI launched a pilot effort in early 2006 and within eight months successfully shared ship position reports from Automatic Identification System (AIS) sources from the United States Navy, the Coast Guard and the Department of Transportation. These vessel reports are **understandable** (i.e., shared using a common information exchange vocabulary), **accessible** (using NCES messaging services), and **visible** (i.e., sources are tagged with discovery metadata which is exploited by a discovery service). Further, the information exchange vocabulary used to share these vessel reports is **governed** by the MDA DS COI Data Management Working Group. Finally, the COI is addressing the need for **trusted** data by including provenance information (e.g., source of data, time of report) in the information exchange vocabulary and developing additional services to perform anomaly detection and identify data discrepancies. This first spiral of capability delivery was a catalyst for change and transformation in the United States Navy. Members of the MDA DS COI believe that the tight scope and focus of the pilot effort, along with engaged executive leadership, were paramount to the pilot's success. For more information, please visit the MDA DS COI web site.[4]

Pilots have proven to be effective as net-centric information sharing pathfinders. Net-centric information sharing pilots can 1) serve as risk reduction for Programs of Record, 2) influence concepts of operation and program requirements, 3) identify and resolve information sharing issues, 4) provide state of the art experimentation, 5) develop and test new approaches, 6) provide a mechanism for user feedback, and 7) provide joint capabilities rapidly. For many programs, implementing net-centric information sharing is new. This can require a change in:

- **Mindset**: From "Need to Know" to "Responsibility to Share"
- **Governance**: From full control to shared capabilities that are jointly managed and funded
- **Policies and Procedures**: For example, accreditation processes that are more flexible and have an enterprise perspective and security policies that accommodate unanticipated users
- **Technologies**: Implementing with Web Services, Service-Oriented Architectures, etc.

Performing a small pilot project can foster these changes and can serve as a pathfinder for subsequent increments of program delivery.

[4] https://mda.spawar.navy.mil

One question often asked is how a program or COI can fund a pilot effort? DoD Instruction 5000.2[5], the definitive DoD acquisition instruction, states that you can use current year funds on pilot demonstrations and risk management to inform the next increment. In other words, a program can reprioritize current capability delivery funds to perform risk reduction on the next increment of capability delivery. Pilot efforts launched as part of a COI often look for additional sources of funding to implement the pilot. However, there is no COI specific funding pool. COIs succeed through the active engagement and commitment of its members and leadership to solve a specific information sharing problem. A COI's authority comes from its membership and leadership. COIs don't directly control resources but COI members and leaders do.

In summary, consider implementing a risk reduction pilot as a pathfinder for net-centric information sharing. This pilot may be executed under the auspices of a COI or as part of a program of record.

Conclusion: A small pilot is an effective mechanism to reduce risk on programs for delivering net-centric information sharing.

RECOMMENDED STEPS

This section outlines recommended steps for implementing net-centric data access services. The steps identified in this paper assume the implementation of a small risk reduction pilot. However, these steps are also applicable to implementing net-centric capabilities on a larger scale through a Program of Record. It is also worth noting that programs can implement net-centric data access services in an incremental fashion.

1. Determine Information Sharing Need and Pilot Scope and Objectives

The first step in implementing net-centric information sharing is to succinctly identify the information sharing problem or need. This information sharing problem must be one which could be aided by sharing data. The DoD DCIO recommends that you define your information sharing need in one sentence. A sample problem statement could be "*Unable to get timely space situational awareness data to support command and control.*"

Once the information sharing problem is defined, you should check to see if other COIs have already solved this problem, a similar problem, or an adjacent problem. You may be able to leverage work already accomplished or join an existing COI. A good starting point for information on current COIs is the COI list included as part of the COI Toolkit that is now available as a link from the left column of the DoD Metadata Registry.[6]

The information sharing need is usually broad enough that it can be broken into increments of capability delivery. The DCIO Data Strategy training recommends that the information need be divided into small increments where each increment of capability delivery (or spiral) is achievable in a short period of time

[5] DoD Instruction 5000.2, May 12, 2003. See paragraphs 3.3.2.1, 3.6.5, and 3.6.6. Available online at: http://www.dtic.mil/whs/directives/corres/html/500002.htm

[6] https://metadata.dod.mil

(e.g., approximately 9 months). The first increment of capability delivery can then be implemented as part of a net-centric pilot.

The first step in implementing a pilot is to scope the effort. Be sure to clearly articulate the pilot scope, objectives and measures of success. You should capture a pilot problem statement as well. A sample pilot problem statement could be "*To reduce the latency of updates to Defense Satellite Communications System (DSCS) Link Status data from 12 hours to 15 minutes, and to provide these updates to authenticated consumers on the SIPRNET via a service interface.*"

We suggest your pilot use a capability based perspective such as the one depicted in figure 3. Begin with your information sharing need which drives the capabilities needed. Your pilot takes the first increment of capability and determines what services are needed to implement that capability. These services require data inputs and provide data outputs. This needed data exchange drives the information exchange vocabulary (IEV) and the implementation. The key message of figure 3 is DO NOT start with the vocabulary or implementation. The IEV and implementation are driven by the needed capability. Previous attempts to build a large, multi-purpose vocabulary by the DoD have failed.[7]

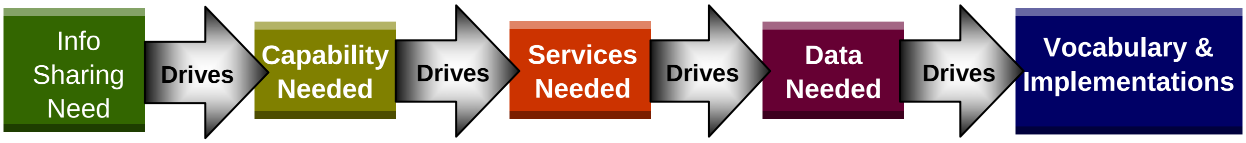


FIGURE 3. CAPABILITY BASED PERSPECTIVE

2. Create Initial Design and Implementation Plan

The next step is to create an initial design and implementation plan. You should begin by developing use cases and scenarios that are based on the pilot problem statement. Using these scenarios, develop a high level architecture that includes definition of planned:

- Services to be implemented
- Data sources
- Information Exchange Vocabulary needs
- Core Enterprise Services usage
- Network on which the data is to be exchanged (e.g., NIPRNET, SIPRNET, JWICS)
- Service interactions to include the tentatively planned information exchange model, e.g.,
    a. Request / Response
    b. Publish / Subscribe
    c. Advertise in combination with Request / Response
- Pilot participants to include what organization will implement the data access services and how the use of these services will be tested (e.g., by what data consumers)
- Security Model

It is strongly recommended that you conduct meetings up front with appropriate data "owners" to obtain approval to access and share data. Sometimes it is challenging to identify what organization is the

[7] Consider DoD Directive 8320.1 Data Administration.

"authoritative owner" of the data. This is the government organization that has the authority to determine what controls are needed to access the data.

Also, because net-centric implementations are relatively new, be sure to engage with the organizations responsible for Information Assurance (IA) on the systems that contain this data. It is helpful to make these IA professionals aware of your information sharing pilot and your anticipated schedule for coming to them to get user and IA concurrence on your planned data access controls. At the conclusion of these early coordination meetings we recommend that you document your agreement on the following:

- The user organization that can make the determination on the needed data access controls,
- Which Designated Approving Authority (DAA) will need to be involved in approving the implementation, and
- A tentative IA approach with suggested timelines.

Your implementation plan must also include the overall pilot plan, budget and milestones. In developing your pilot implementation plan, clearly articulating the scope of the effort is key. If the pilot is too ambitious to accomplish in nine months or less, you may want to consider sequencing the capabilities into several iterations (or spirals) to implement and extend the solution. Be sure to establish target milestones and, where possible, synchronize with joint exercises, programs of record incremental delivery cycles, and requirements, acquisition and budgeting cycles. Identify funding requirements for personnel, hardware, software, and other resources. Finally, be sure to include a pilot transition plan to include determination of the organization that would develop and maintain an operational version of the piloted data access services.

Scope is key!

3. Obtain Approval of Plan and Secure Funding

Once you have your initial design and proposed implementation plan, you must obtain approval to proceed and secure the pilot funding. The pilot funding generally comes from existing programs of record but other sources may be available. Obtain approval on the implementation plan including the:

- Data access approach
    a. What data will be made available
    b. Agreement that planned data access controls suffice
    c. Who has decision authority on determining the planned access controls
- Certification and Accreditation (C&A) approach
- Schedule and milestones
- Targeted transition plan
- Budget and source of funding

Usually pilots are executed through a partnership with a program of record, operational users, and other members of the COI. Sometimes this results in prioritizing current year program funds to perform risk reduction on the next program increment. In this case, the Program Manager must agree that the pilot provides risk mitigation for the next program increment to ensure commitment and appropriate priority for the effort.

4. Develop and Coordinate Information Exchange Vocabulary (IEV)

As previously noted, the services to be developed will require data inputs and data outputs. These data exchanges must be documented and agreed upon. Key data exchanges should be captured in an agreed upon information exchange vocabulary (IEV).

There are three key steps in developing an IEV. The first step is to be sure to involve all the key stakeholders in the development and/or review of the IEV. Key stakeholders and their role relative to the IEV are shown in table 1.

TABLE 1. IEV STAKEHOLDER ROLES

Stakeholder	Stakeholder Role
Decision Makers	Ensure all the right players are involved including both providers and consumers of this information
Operators and Users	Ensure the planned capabilities will meet operational needs and share the “right” information
Data Owners	Tag data. Determine access rules and attributes required to implement the access rules.
Program Managers	Ensure the resulting IEV will meet program needs for sharing the relevant data and plan for the use of the resulting IEV
Engineers and Developers	Ensure data schema is easy to implement and doesn’t use features not supported by current tools
Subject Matter Experts	Ensure the IEV is capturing the relevant information to the right level of precision and includes necessary provenance data

The next step is to create the information exchange vocabulary needed to support the planned services. We recommend that you follow a systematic approach by beginning with modeling the use cases and scenarios, developing a logical data model to support those scenarios, and deriving physical schemas and data definitions from the logical model. Be sure to capture both the data syntax (i.e., data structure) and the data semantics (i.e., data meaning). The IEV development team should reuse existing data models and schemas, where appropriate. This includes using the DoD and IC Universal Core vocabulary[8] where appropriate to facilitate cross domain information sharing. Another resource for locating relevant structural metadata that could be reused is the DoD Metadata Registry.[9] You should consider how much provenance information (e.g., data source, time data collected or shared) you wish to capture in your IEV.

Finally, recognize that vocabulary development and maintenance is an iterative process. While your stakeholder community may agree upon an IEV to support a specific set of services to build a particular capability, the vocabulary is bound to evolve as experience is gained and needs change.

Development, stewardship and enforcement of community agreed upon IEVs are tasks where COIs can play an important role. The COI leadership can ensure all the right stakeholders are involved and

[8] The Universal Core will soon be posted to the DoD Metadata Registry (metadata.dod.mil)
[9] https://metadata.dod.mil

can enforce use of the IEV for information sharing. The COI can also provide governance for the evolution of the IEVs.

5. Implement the Pilot

Once you have approval and funding on your initial design, it is time to begin the detailed design and development planning. This implementation step can proceed in concert with the development of the IEV. There are seven key steps in implementing the net-centric data access services.

Design Service Interfaces and Interactions

The first step is to decompose the high level architecture into a detailed design to include service interfaces and interactions. The specification of the service interface should incorporate the approved IEV. The detailed design must also address how to integrate with authoritative data sources to include planned security approaches. One essential step in defining the security approach is to determine the access rules and attributes needed to implement the access rules. Plans for use of the DISA provided Core Enterprise Services (CES) should be documented as well.

Develop Implementation and Deployment Plan

Another step is to develop an implementation and deployment Plan of Action and Milestones (POA&M). Where the data access services are to be deployed on a classified network, it is usually advisable to implement initially on an unclassified network (with simulated data if necessary) before deploying to a classified system. This allows one to test and troubleshoot the external interfaces on an unclassified network.

Develop Information Assurance (IA) Approach

To ensure that the requirements of the Federal Information Security Management Act (FISMA) are either met or exceeded, DoD entities must follow the DoD Information Assurance Certification and Accreditation Process (DIACAP).[3] DIACAP establishes an information system certification and accreditation (C&A) process to manage the implementation of Information Assurance capabilities and services and provide visibility of accreditation decisions regarding the operation of DoD information systems, including core enterprise services and other services-based software systems and applications. This process encompasses the system’s life cycle. As part of this process, you must work with the Designated Approving Authority (DAA). This is the official with the authority to assume responsibility for an acceptable level of risk for a given system. We recommend you involve the relevant DAA (or DAAs) for your pilot as early in the process as possible to discuss with them your planned approach and confirm the C&A approach to be used along with the associated timelines for each step in this C&A process.

Define Sample Information Presentation of Net-Centric Data

Another step in the process is to think about how the data made available by the service will be integrated into an operator’s current information environment. This step can involve human-systems integration (HSI) analyses to determine information needs and information tiers (primary, secondary) of known or expected users of the data. For example, a common HSI methodology, the Cognitive Work Analysis, can be used to characterize the target user’s current information environment, tasks, and decisions. The findings can then be used to create a sample consolidated display that integrates native data from the user’s local systems with the external data from net-centric data service. The sample display can be used to collect feedback from target users (e.g., completeness of information, level of detail, level of access) and refine the set of data to be made available by the data service.

Implement Data Services

After you complete the detailed design and document and approve the implementation and deployment plan, you must implement the pilot capabilities. It is important that you leverage industry standards and design patterns where possible.

Test Pilot

Testing is a fundamental part of any development effort. Your test plan should include unit testing, performance testing, and user tests. Testing must occur both in the development environment and again when deployed to the demonstration environment. In fact, new Test and Evaluation (T&E) policy revisions direct that T&E should assess improvements to mission capability and operational support based on users needs and should be reported in terms of operational significance to the user.[10] For pilot efforts, aligning your schedule to allow leveraging a user test or exercise is an expedient way to get user feedback on the developed capabilities.

Register IEV, Content and Services for Discovery

A key step in making data and services visible, accessible, and understandable is to register your artifacts for discovery using the Core Enterprise Services provided by DISA. The IEV should be registered in the DoD Metadata Registry to allow it to be discovered and used. The software services should be registered in the DoD Service Registry to make them discoverable. Finally, describe the content available in the DoD Enterprise Catalog using the DoD Discovery Metadata Specification (DDMS). This is akin to placing an entry in a card catalog. The details of how to perform these steps are available from the NCES home page.[11]

6. Demonstrate and Evaluate the Pilot

Once the pilot capabilities are implemented and tested, they are ready to be demonstrated. The ideal case is for the capabilities to be demonstrated as part of a joint exercise. This is usually less intrusive than orchestrating a pilot specific demonstration and it often provides more meaningful user feedback.

A key step in any risk reduction pilot effort is to document the user feedback received as well as any lessons learned. There may be lessons learned regarding the pilot experience itself, use of the IEV, the specific capabilities developed, or desired enhancements. These results are valuable inputs to all stakeholders but especially to any relevant programs who may implement using the developed IEV, the programs that may be asked to operationalize the piloted capability as captured in the pilot transition plan, or any potential consumers who may use these capabilities when they are made available operationally.

Finally, the pilot should be evaluated against the metrics or success criteria determined at the start of the process. This self-assessment step will determine the subsequent steps (e.g., implement the next pilot spiral, transition the pilot to operations, document new program requirements).

[10] Office of the Secretary of Defense, *Test and Evaluation Policy Revisions,* December 22, 2007. Available online at: https://akss.dau.mil/Documents/Policy/TE-Policy-Memo-Dec-2007.pdf

[11] http://www.disa.mil/nces/nces

7. Transition the Pilot

A pilot transition plan should be created as part of the early pilot planning. This transition plan should identify the targeted program of record that would make the piloted capabilities available operationally if they prove to have operational value. This step assumes that the user feedback indicated that the developed capabilities indeed had operational value and should be transitioned to operations. Therefore, this step is to integrate pilot results with the targeted Programs of Record as defined in the pilot transition plan. The pilot team should document what would be needed to make the pilot capabilities operational including any remaining capability gaps. While the transition plan may have identified tentative funding avenues, it is when actually implementing the transition plan that the requirements will be incorporated into the relevant program Capability Development Documents (CDDs) and actual resource needs and avenues will be identified.

8. Implement the Next Spiral (if appropriate)

Another necessary step is assessing whether the information sharing problem has been solved. If transitioning the capabilities developed as part of the risk reduction pilot does not address all aspects of the information sharing problem, then one must assess whether to tackle the next increment of needed capability.

KEY REFERENCES

1. DoD Directive 8320.2, *Data Sharing in a Net-Centric Department of Defense*, December 12, 2004. Establishes policies and responsibilities to implement data sharing, in accordance the DoD Net-Centric Data Strategy and directs the use of resources to implement data sharing among information capabilities, services, processes, and personnel interconnected within the Global Information Grid (GIG).

2. DoD 8320.2-G, *Guidance for Implementing Net-Centric Data Sharing*, April 12, 2006. Issued under the authority of DoD Directive 8320.2, contains guidance for the community-based transformation of existing and planned information technology (IT) capabilities across the Department of Defense (DoD) in support of Department-wide net-centric operations.

3. DoD Instruction 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*, 28 Nov 2007.

4. DoD Net-Centric Data Strategy, May 9, 2003. Outlines the vision for managing data in a net-centric environment by ensuring that it is visible, accessible, understandable, trusted and governable.

5. DoD Net-Centric Data Strategy / COI Training. Training materials are available on Defense Knowledge Online (DKO) at: https://www.us.army.mil/suite/kc/8090086 A DKO account is required.

6. DoD / IC Net-Centric Services Strategy, July 2007. Describes the DoD and Intelligence Community (IC) vision for a net-centric environment that increasingly leverages shared services and Service Oriented Architecture. It builds upon the DoD Net-Centric Data Strategy's (May 2003) goals of making data assets visible, accessible, and understandable. This strategy establishes services as the preferred means by which data producers and capability providers can make their data assets and capabilities available across the DoD and beyond. It also establishes services as the preferred means by which consumers can access and use these data assets and capabilities.

7. Net-Centric Core Enterprise Services (NCES) Program. Publicly accessible web page that contains an NCES overview briefing and the NCES Users Guide.

8. The Power of Information. DoD Chief Information Officer Pamphlet, 2006.